Amendments to the Specification:

Please amend the paragraph beginning at page 5, line 12 as follows:

In these various configurations, hardfile 105 includes non-volatile memory for storing an operating system used by computer system 100, and typically user data and application software. Most commonly, hardfile 105 is a fixed ~~harddrive~~ hard drive storing the information on magnetic media. Computer system 100 includes a ~~harddrive~~ hard drive adapter for controlling the storage and retrieval when hardfile 105 is a ~~harddrive~~ hard drive. Computer system 100 will typically include other control and data interfaces when hardfile 105 is not a ~~harddrive~~ hard drive, but adapting the present invention to such alternate hardfile systems is within the skill of a person of ordinary skill in the art and would be achieved from this disclosure without undue experimentation. To simplify the discussion, the preferred embodiment will be described in the case that hardfile 105 is a ~~harddrive~~ hard drive.

Please amend the paragraph beginning at page 5, line 22 as follows:

In the preferred embodiment, hardfile 105 complies with applicable standards for an ATA/ATAPI-4 (NCITS 314-1998) or later compliant ~~harddrive~~ hard drive, the standard hereby expressly incorporated by reference for all purposes. Hardfile 105 must include at least one partition, and in some cases, there may be multiple logical partitions accessible to computer system 100. In the ATAPI-4 standard, hardfile 105 may be established optionally with an additional partition referred to as a Protected Area Run Time Interface Extension Services or simply PARTIES partition prior to loading the operating system. The PARTIES partition often is set by computer system 100 using a firmware interface (PARTIES) for controlling and accessing this PARTIES partition, and is invisible or otherwise non-accessible to most conventional computer subsystems or conventional routines of the operating system. The PARTIES partition is used to

store administration or non-user data. ATAPI-4 provides a procedure called SETMAX that adjusts the size of this PARTIES partition. The preferred embodiment of the present invention uses this SETMAX procedure in a way not contemplated by the standard to provide a novel use of the PARTIES partition to secure data. NCITS can be reached at www.ncits.org.

Please amend the paragraph beginning at page 6, line 20 as follows:

In the event that the POST detects a special ~~pre-boot~~ boot condition, computer system 100 dynamically adjusts SETMAX to exclude all or a portion of hardfile 105 from access by the operating system. The special boot condition may be any type of hardware, software or firmware condition that, in the particular application, would suggest limiting access to part of hardfile 105.

Please amend the paragraph beginning at page 8, line 23 as follows:

If the test at step 305 is yes, computer system 100 sets the configuration parameter of hardfile 105 to the appropriate level, given the detected ~~pre-boot~~ boot condition. For example, if a hardware tamper is detected and hardfile 105 is an IDE/ATAPI-4 ~~harddisk~~ hard drive, computer system 105 sets SETMAX to a smaller size than the full readable size of the ~~harddisk~~ hard drive and limits the size to a minimum for operating system access. If for example the boot condition is a clearing of a previous tamper condition and hardfile 105 is an IDE/ATAP-4 ~~harddisk~~ hard drive, computer system 100 sets SETMAX to be larger and include more of hardfile 105 for access.

Please amend the paragraph beginning at page 9, line 11 as follows:

While the preferred embodiment has been described in terms of a dual operational mode for hardfile 105, the present invention is not so limited. In some applications, it may be desirable or beneficial to provide for three or more operational modes of hardfile 105. In this application,

various ~~pre-boot~~ boot conditions may lead to degrees of access to user data or software applications. In some embodiments, user credentials being made available before the SETMAX value is established can provide for increased data security over user/permission based access systems.